W19D1

Il sistema di valutazione delle minacce di **ThreatConnect** si basa su una scala a 6 livelli, da 0 a 5, che valutano la pericolosità di un indicatore. Questi livelli sono:

1. **Sconosciuto (0)**: Non ci sono abbastanza informazioni per valutare il livello di minaccia.
2. **Sospetto (1)**: Attività sospette sono state osservate, ma non c'è conferma di attività dannosa.
3. **Basso (2)**: La minaccia rappresenta un avversario non sofisticato, di natura opportunistica e temporanea, legata a tentativi pre-attacco.
4. **Moderato (3)**: Rappresenta un avversario capace, con azioni dirette ma non persistenti. Tipicamente collegato alla fase di consegna, sfruttamento o installazione di un attacco.
5. **Alto (4)**: Coinvolge un avversario avanzato e indica attività mirate e persistenti, con una compromissione già avvenuta (come il comando e controllo).
6. **Critico (5)**: Rappresenta una minaccia da parte di un avversario altamente qualificato e ben finanziato, con capacità illimitate e determinazione completa. Può verificarsi in qualsiasi fase dell'intrusione.

Questa scala permette di classificare in modo sistematico la gravità delle minacce per facilitare le azioni di risposta.

FACOLTATIVO

Ecco un elenco di minacce informatiche comuni che possono colpire un'azienda, basato su un'analisi delle minacce più diffuse e i loro potenziali impatti:

1. **Phishing**: Una delle minacce più diffuse e durature, il phishing coinvolge l'inganno delle vittime tramite email, messaggi o link che sembrano legittimi, inducendole a fornire informazioni sensibili come credenziali di accesso o dettagli finanziari. Le tecniche di phishing si evolvono continuamente, includendo anche truffe più sofisticate come il *spear phishing* (mirato a individui specifici) o *vishing* (via telefonica)
2. **Malware**: Il termine "malware" include vari tipi di software dannosi, come virus, trojan, ransomware e spyware, progettati per danneggiare, rubare dati o prendere il controllo di sistemi informatici. Il malware può diffondersi attraverso allegati email, download non sicuri o vulnerabilità di sicurezza non corrette
3. **Attacchi DDoS (Distributed Denial of Service)**: Questi attacchi mirano a sovraccaricare i server con un'enorme quantità di traffico dannoso, rendendo i servizi online indisponibili. Sebbene non comportino necessariamente furto di dati, possono causare gravi danni reputazionali e interrompere le operazioni aziendali
4. **Ransomware**: In un attacco ransomware, gli hacker bloccano l'accesso ai dati aziendali crittografandoli e chiedono un riscatto per restituire il controllo. Questo tipo di attacco è particolarmente devastante poiché può portare a perdite finanziarie considerevoli e interruzioni operative

5. **SQL Injection**: Questo tipo di attacco sfrutta vulnerabilità nei database, inserendo codice SQL dannoso per ottenere l'accesso non autorizzato ai dati sensibili. Le conseguenze possono includere il furto di dati o il controllo completo dei sistemi
6. **Attacchi Man-in-the-Middle (MITM)**: Gli attacchi MITM intercettano le comunicazioni tra due parti, permettendo all'aggressore di manipolare o rubare informazioni. Spesso vengono condotti tramite reti Wi-Fi non sicure o vulnerabilità SSL
7. **Cross-Site Scripting (XSS)**: XSS è una vulnerabilità delle applicazioni web che consente l'inserimento di script dannosi nelle pagine web visualizzate dagli utenti. Questo tipo di attacco può essere utilizzato per rubare informazioni personali o manipolare sessioni di autenticazione
8. **Insider Threats (Minacce interne)**: Gli attacchi interni sono perpetrati da individui all'interno dell'azienda, che sfruttano l'accesso privilegiato per compromettere la sicurezza. Le motivazioni possono variare dal profitto personale alla vendetta o alla semplice negligenza

Queste minacce dimostrano la necessità per le aziende di adottare misure di sicurezza solide, come formazione sulla sicurezza per i dipendenti, l'implementazione di software di sicurezza avanzati e l'aggiornamento regolare delle infrastrutture IT per mitigare questi rischi.